کرپٹو جیکنگ

بزنس ماڈل یا چوری کی نئی قسم؟

ڈاکٹر مبشر حسین رحمانی

منسٹر ٹیکنالوجیکل یونیورسٹی، آئرلینڈ

کرپٹو جیکنگ

بزنس ماڈل یا چوری کی نئ قسم؟

ڈاکٹر مبشر حسین رحمانی

منسٹر ٹیکنالوجیکل یونیورسٹی، آئرلینڈ

کرپٹو جیکنگ: بزنس ماڈل یا چوری کی نئ قسم؟

آپ نے "بغیر کام کئے کمانا" جسے Passive Income بھی کہا جاتا ہے کے بارے میں تو سنا ہی ہو گا جس میں کسی چیز میں ابتدائی سرمایہ کاری کر دی جاتی ہے اور پھر مستقبل میں پیسے یعنی نفع ملتا رہتا ہے۔ جی ہاں، اسی سوچ کو ذہن میں رکھتے ہوئے ایک سائنسی تحقیق کے مطابق سائبر کرمنلز نے اوسطاً ایک مہینے میں اکتالیس ہزار امریکی ڈالر کمائے جو کہ ماہانہ تقریباً نوے لاکھ پاکستانی روپے بنتے ہیں۔ کچھ دیگر سائبر کرمنلز نے اوسطاً بارہ لاکھ امریکی ڈالر تک کمائے جو کہ تقریباً چھبیس کڑور پاکستانی روپے ماہانہ بنتے ہیں۔ یہ کمائی ان سائبر کرمنلز نے کرپٹو جیکنگ Cryptojacking کی مدد سے کی جسے ڈرائیو بائی مائننگ Drive-by Mining بھی کہا جاتا ہے۔ کرپٹو جیکنگ کیا ہے؟ کیسے کام کرتی ہے؟ ان سائبر کرمنلز نے اس سے اتنا پیسہ کیسے کمالیا؟ کیا ہم بھی کرپٹو جیکنگ کا دانستہ یا نادانستہ شکار بن سکتے ہیں؟ کیا مستقبل میں کرپٹو جیکنگ کو ایک نئے بزنس ماڈل یعنی اشتہارات کے متبادل کے طور پر بھی استعمال کیا جا سکتا ہے؟

ہم میں سے ہر ایک نے ہوائی جہاز کی ہائی جیکنگ سے متعلق تو سنا ہی ہو گا اور ہمیں بالکل واضح ہے کہ ہوائی جہاز کا اغوا کرنا اور پھر اس کو اپنے مذموم ذاتی مقاصد کی تکمیل کیلئے استعمال کرنا ملکی اور بین الاقوامی قوانین کے لحاظ سے جرم ہے۔ نیز شریعتِ مطہرہ بھی کسی کی چیز کو بغیر اُسکے مالک کی اجازت کے استعمال کرنے سے منع کرتی ہے۔ بس یہی کچھ حال کرپٹو جیکنگ کا بھی ہے جس کے اندر کسی صارف کے کمپیوٹر یا موبائل کو بغیر اُسکی اجازت کے کرپٹو کرنسی کی مائننگ کے عمل میں استعمال کیا جاتا ہے اور کرپٹو کرنسی کی مائننگ کے عمل سے جو نفع حاصل ہوتا ہے وہ کرپٹو جیکنگ کرنے والے رکھ لیتے ہیں۔

کرپٹو کرنسی مائننگ کا عمل بہت منافع بخش ہے مثلاً بٹ کوائن مائننگ پر سوا چھ بٹ کوائن انعام ملتا ہے جو کہ آج کے ریٹ کے حساب سے تقریباً دو کڑور اسی لاکھ پاکستانی روپے بنتے ہیں۔ کرپٹو کرنسی مائننگ مختلف طریقہ کار سے کی جا سکتی ہے مثلاً کوئی شخص انفرادی طور پر اپنے ذاتی کمپیوٹر یا موبائل فون سے بھی مائننگ کر سکتا ہے مگر اس طریقے سے نفع کمانے کے مواقع تقریباً نہ ہونے کے برابر ہیں۔ دوسرا رائج طریقہ یہ ہے کہ کوئی شخص اپنے ذاتی کمپیوٹر کو مائننگ پول کا حصہ بنادے اور پھر مائننگ پول اگر مائننگ کے عمل میں کامیاب ہو جائے تو اس کو جو منافع ملے وہ صارف کو بھی دے دے۔ تیسرا یہ کہ سائبر کرمنلز خفیہ طور پر آپ کے کمپیوٹر کو استعمال کرتے ہوئے کرپٹو مائننگ کا عمل کروائے اور پھر خود منافع حاصل کرلے۔ عملی طور پر کرپٹو جیکنگ کرنے والے دنیا میں ہزاروں لاکھوں کی تعداد میں کمپیوٹرز سے بیک وقت مائننگ کا عمل کرواتے ہیں یا انہیں مائننگ پول سے جوڑ دیتے ہیں جس کے نتیجے میں اُن کے پاس اتنی کمپیوٹیشنل پاور آجاتی ہے جس سے وہ کرپٹو کرنسی مائننگ کا عمل تسلی بخش طریقے سے کرسکیں۔

سائبر کرمنلز کو کرپٹو جیکنگ کرنے سے ایک فائدہ تو یہ ہے کہ ان کو مائننگ ہارڈ وئیر پر سرمایہ کاری نہیں کرنی پڑتی جس سے ان کی سرمایہ کاری اور آپریشنل اخراجات نہ ہونے کے برابر ہو جاتے ہیں۔ آپ اندازہ کیجئے کہ اس وقت اوسطاً ایک مائننگ کی مشین تقریباً چھ ہزار امریکی ڈالر کی ملتی ہے جو کہ بارہ لاکھ پاکستانی روپے بنتے ہیں اور اگر پورا کنٹینر ان مائننگ ڈیوائسس کا لیا جائے تو تقریباً ایک لاکھ دس ہزار امریکی ڈالر کا ملتا ہے جو کہ سوا دو کروڑ پاکستانی روپے بنتے ہیں۔ نیز دوسرے سائبر حملوں کے مقابلے میں کرپٹو جیکنگ زیادہ پرکشش ہے کیونکہ سائبر حملوں سے حفاظت کرنے والی سائبر سیکورٹی کمپنیاں اور ادارے رینسم وئیر Ransomware پر توجہ مرکوز رکھتے ہیں۔ رینسم وئیر اُن سائبر حملوں کو کہا جاتا ہے جس میں سائبر حملہ آور سائبر حملوں کے ذریعے متاثرین سے تاوان وصول کرتے ہیں۔ جبکہ کرپٹو جیکنگ کے اندر کوئی تاوان تو وصول نہیں کیا جاتا البتہ دوسرے کے کمپیوٹر کو استعمال کرتے ہوئے کرپٹو کرنسی مائننگ کی جاتی ہے جو کہ صارفین کیلئے فوراً اتنی نقصان دہ نہیں ہوتی جتنا کہ دوسرے سائبر حملے جن کے اندر یا تو صارف اپنا پورا ڈیٹا ہی ضائع کر دیتا ہے یا پھر اُسے تاوان دینا پڑتا

ہے۔ سائبر کرمنلز کے نفع کے بالمقابل عام صارفین کو کرپٹو جیکنگ سے جو نقصان ہوتا ہے اُن میں ان کے ہارڈویئر کی اوورہیٹنگ ہے اور دوسرا اُن کے مائیکروپروسیسر کی کارکردگی میں کمی ہے۔

بنیادی طور پر کرپٹو جیکنگ کے کام کا طریقہ کار یہ ہوتا ہے کہ کسی ویب سائٹ پر کرپٹو جیکنگ اسکرپٹ رکھا جاتا ہے۔ پھر جب بھی کوئی صارف اس ویب سائٹ پر آتا ہے تو ویب سائٹ آرکیسٹریٹر اسکرپٹ Orchestrator Script چلاتا ہے جو کہ آنے والے صارف کے کمپیوٹر کی جانچ کرتا ہے کہ اس میں کون سا آپریٹنگ سسٹم OS انسٹال ہے اور کتنے سی پی یو کے کور CPU Core قابل استعمال ہیں۔ صارف کے کمپیوٹر کی جانچ پڑتال کے بعد ایک باہر کے کمپیوٹر سرور Server سے یا اسی ویب سائٹ سے کرپٹو مائننگ پے لوڈ Mining Pay Load صارف کے کمپیوٹر پر ڈاؤنلوڈ کر دیا جاتا ہے۔ اس کے بعد کوڈ کے چھوٹے چھوٹے حصے جنہیں تھریڈ Thread بھی کہا جاتا ہے صارف کے کمپیوٹر پر چلائے جاتے ہیں اور پھر اس صارف کے کمپیوٹر کا کنکشن مائننگ پول کے سرور سے ویب ساکٹ کی مدد سے جوڑ دیا جاتا ہے۔ اور پھر جو مائننگ کا عمل اس صارف کو کرنا ہے وہ مائننگ پول سے حاصل کر کے اس کو پایہ تکمیل تک پہنچاتا ہے اور مطلوبہ ہیش Hashes کو ویب ساکٹ کی مدد سے مائنگ پول پر واپس اپ لوڈ کر دیا جاتا ہے۔ عمومی طور پر سٹرائم Stratum پروٹوکول کو ان مقاصد کیلئے استعمال کیا جاتا ہے۔ اوراس طریقے سے کسی دوسرے کے کمپیوٹر کو استعمال کرتے ہوئے کرپٹو جیکنگ کی جاتی ہے۔

ٹڈبٹ TidBit نے سن ۲۰۱۳ میں براؤزر بیسڈ مائننگ کی شروعات کی جس کا کوڈ ایم آئی ٹی کے طالبعلموں نے لکھا۔ اسی طرح کوائن ہائیو CoinHive کرپٹو جیکنگ کے تناظر میں بہت مشہور ہوا۔ کوائن ہائیو ایک جاوااسکرپٹ ویب سائٹ والوں کو دیتی تھی تاکہ ویب سائٹ والے اس کوڈ کو اپنی ویب سائٹ پر استعمال کر سکیں۔ پھر جب بھی کوئی صارف اُن کی ویب سائٹ پر آئے تو وہ خفیہ طور پر اپنی ویب سائٹ پر آنے والوں کی اجازت کے بغیر اس کے کمپیوٹر کو استعمال کرتے ہوئے کرپٹو کرنسی مائن کرلیں۔ ٹرینڈ مائیکرو Trend Micro کمپنی نے کوائن ہائیو CoinHive کرپٹو جیکنگ مال ویئر کو سب سے پہلے ڈھونڈا تھا۔ دنیامیں مشہور کرپٹو مائننگ سروسز ہیں ان میں DeepMiner,

Coinhive, Minr, JSECoin, CoinImpوغیرہ شامل ہیں۔ مونیرو Monero اور بٹ کوائن Bitcoin وہ کرپٹو کرنسیاں ہیں جن کی مائننگ سب سے زیادہ کرپٹو جیکنگ کی مدد سے کی گئی۔

کرپٹو جیکنگ مختلف طریقوں سے کی جاسکتی ہے مثلاً کمپیوٹر براؤزر کی مدد سے، اینڈرائڈ ایپلیکشنز کی مدد سے، تھرڈ پارٹی لائبریری کی مدد سے، براؤزر ایکسٹینشن کی مدد سے، راؤٹرز کی مدد سے یا بوٹ نیٹ کی مدد سے۔ ان سب میں براؤزر بیسڈ کرپٹو جیکنگ سب سے مشہور ہے اور صارف کا براؤزر جتنی دیر کھلا رہے گا اتنی دیر کرپٹو مائننگ اسکرپٹ چلتا رہے گا اور کمپیوٹر مائننگ کے عمل میں مصروف رہے گا۔

کمپیوٹر کی دنیا میں سائبر حملے عام ہیں۔ ان سائبر حملوں کی مختلف اقسام ہیں اور ان میں سے ایک اہم قسم مال ویئر کی ہے۔ مال ویئر وہ سافٹ ویئر ہوتے ہیں جو کہ آپ کے کمپیوٹر پر انسٹال ہو جاتے ہیں اور پھر آپ کے کمپیوٹر کو نقصان پہنچاتے ہیں۔ روایتی طور پر مال ویئر لانچ کرنے کیلئے کوئی فائل آپ کے کمپیوٹر پر انسٹال کرنی پڑتی ہے اور پھر وہ مسائل پیدا کرتی ہے مگر اب نئے قسم کے مال ویئر آگئے ہیں جن کو فائل لیس مال ویئر کہا جاتا ہے۔ یعنی اب ہیکر یا سائبر کرمنل کو آپ کے کمپیوٹر پر حملہ کرنے کیلئے کوئی فائل یا سافٹ ویئر انسٹال کرنے کی ضرورت نہیں ہے بلکہ براؤزر کی مدد سے آپ کے کمپیوٹر پر حملہ کر سکتا ہے۔ یعنی فائل لیس مال ویئر کے اندر کمپیوٹر پر موجود سافٹ ویئر کو استعمال کرتے ہوئے مذموم مقاصد کیلئے استعمال کیا جاسکتا ہے۔ کرپٹو جیکنگ بنیادی طور پر ایک مال ویئر ہے۔ سن ۲۰۲۰ میں تمام سراغ لگائے گئے مال ویئر میں اکتالیس فیصد کرپٹو جیکنگ کا مال ویئر تھا۔ اس سے اندازہ کیا جاسکتا ہے کہ اس کرپٹو جیکنگ مال ویئر کا کتنا وسیع استعمال ہو تا رہا ہے۔ یعنی اب ہیکر یا اٹیکر کو آپ کے کمپیوٹر پر کوئی فائل انسٹال کرنے کی ضرورت نہیں ہے بلکہ اب وہ آپ کے کمپیوٹر براؤزر کی مدد سے آپ کے کمپیوٹر پر اٹیک کر سکتا ہے۔ کرپٹو جیکنگ نے ہیکنگ کی دنیا میں ہیکرز کیلئے نئے مواقع کھولے ہیں کہ کسطرح سے نئے اقسام کے سائبر حملے کئے جاسکتے ہیں۔

حالیہ تاریخ میں میکروٹیک راؤٹرز MikroTik Routers کرپٹو جیکنگ سائبر حملے سے شدید متاثر ہوئے۔ انٹرنیٹ ٹریفک جو ان راؤٹرز سے گزرتا ہے ان میں ہر باہر جانے والے کنکشن

میں کرپٹو جیکنگ اسکرپٹ شامل کر دیا گیا۔ اس کے نتیجے میں ہر ویب سائٹ کوئی بھی صارف استعمال کرے گا جو کہ ان کے راؤٹرز سے لنک ہو وہ ان چوروں کو مائننگ کے نتیجے میں نفع پہنچائے گا۔ اس سائبر حملے میں سائبر کرمنلز کے پاس دس لاکھ سے زیادہ راؤٹرز کا کنٹرول تھا جو کہ تقریباً ستر فیصد دنیا بھر میں لگائے گئے راؤٹرز ہیں۔ انہی راؤٹرز کی مدد سے اوسطاً بارہ لاکھ امریکی ڈالر ماہانہ نفع کمایا گیا جو کہ ویب سائٹ بیسڈ کرپٹو جیکنگ کی مدد سے صرف اکتالیس ہزار امریکی ڈالر بنتا ہے۔ اس سائبر حملے کی شدت کا اندازہ اس بات سے کر سکتے ہیں کہ کچھ ویب سائٹ کے بجائے یہاں پر دس لاکھ سے زیادہ راؤٹرز ہیں جو کہ اس کرپٹو جیکنگ کے حملے سے متاثر ہوئے۔

کرپٹو جیکنگ سے بچنے کا ایک طریقہ کار یہ ہے کہ ہم اپنے کمپیوٹر پر ویب براؤزر پر جاوا اسکرپٹ کی تمام ایپلیکیشنز کو بند کر دیں۔ اس کا نتیجہ یہ ہو گا کہ کرپٹو مائننگ کا سیشن ختم ہو جائے گا۔ دوسرا طریقہ یہ ہے کہ ہم ٹاسک مینیجر میں دیکھیں کہ کتنے پروسسز چل رہے ہیں اور وہ کتنی سی پی یو کی پروسیسنگ پاور کو استعمال کر رہے ہیں اور پھر غیر ضروری پروسسز کو ختم کر دیا جائے۔ تیسرا طریقہ کار کرپٹو جیکنگ سے بچنے کا یہ ہے کہ ہم مال وئیر بائٹ Malwarebytes سافٹ وئیر اپنے کمپیوٹر پر انسٹال کریں جس کی مدد سے ہم اس طرح کے تمام مال وئیر ز سے بچ سکتے ہیں اور جو ہمیں آگاہی دے سکتا ہے کہ کون سی ویب سائٹ پر جانا رسکی ہو سکتا ہے۔

کرپٹو جیکنگ کا ایک متوقع استعمال ایک نئے بزنس ماڈل کے طور پر بھی پروان چڑھ رہا ہے اور وہ یہ کہ مروجہ طریقہ کار ویب سائٹ کا نفع کمانے کا یہ ہوتا ہے کہ ویب سائٹ پر اشتہارات ہوتے ہیں اور کوئی بھی صارف جو ان ویب سائٹ پر آئے گا وہ ان اشتہارات پر کلک کرے گا تو ویب سائٹ والوں کو منافع ملے گا اور اس کی مختلف اسکیمیں متعارف ہیں۔ کرپٹو جیکنگ کرنے والی بعض کمپنیاں اب صارف سے اجازت لیتی ہیں کہ اگر آپ کے کمپیوٹر براؤزر کو استعمال کرتے ہوئے ہم کرپٹو کرنسی مائننگ کا عمل کریں تو اس پر آپ کو انعام دیا جائے گا جیسے رعایت، پریئیم فیچر، کریڈٹ وغیرہ۔ نیز اگر کرپٹو جیکنگ کو اشتہارات کے متبادل کے طور پر استعمال کیا جائے یعنی ویب سائٹ کے مالکان منافع کمانے کے بجائے مختلف اشتہارات کی مہم مثلاً بینر ایڈز یا پے پر کلک والے اشتہارات

استعمال نہ کریں بلکہ وہ ان تمام اشتہارات کو اپنی ویب سائٹ سے ہٹا دیں اور اُن کی جگہ کرپٹو جیکنگ کے اسکرپٹ کو استعمال کریں اور وہ با قاعدہ ویب سائٹ پر آنے والے صارفین سے اس کے متعلق اجازت بھی لے لیں تو سوال یہ پیدا ہوتا ہے کہ کیا اس طریقے سے کرپٹو جیکنگ سے پیسہ کمانا جائز ہے ؟

اگر صارفین سے اجازت لی بھی جائے تو عام صارفین کو اس کی تکنیکی تفصیلات کا علم نہیں ہوتا لہذا اجازت لینا نہ لینا برابر ہی ہوتا ہے۔ اور اس کی بنیادی وجہ یہ ہے کہ کچھ صارفین کو اس کا اندازہ ہی نہیں ہوتا کہ وہ کس بات کی اجازت دے رہے ہیں اور ان کو مقابل میں کیا ملے گا۔ مثلاً جو کمپیوٹر استعمال کرتے ہیں وہ کوکیز کے نوٹس کو بغیر پڑھے ہی تسلیم کر لیتے ہیں اور یہی کچھ حال کرپٹو جیکنگ کی صارفین سے اجازت لینے کی بھی شکل ہے۔ کرپٹو جیکنگ کو اشتہارات کے متبادل کے طور پر استعمال کرنے کے بارے میں مفتیانِ کرام یہ ارشاد فرماتے ہیں کہ ایسا کرنا جائز نہیں۔ یہ اسی طرح ہے کہ کوئی اپنی ویب سائٹ سے ناجائز اشتہارات مثلاً شراب کے اشتہارات استعمال کرکے پیسے کمائے لہذا جس طریقے سے ایسے اشتہارات سے نفع کمانا جائز نہیں بِعَینہٖ اسی طریقے سے کرپٹو جیکنگ کے اشتہارات کے متبادل کے طور پر استعمال کرنا اور اس سے نفع کمانا جائز نہیں۔

خلاصہ یہ کہ کسی کے گھر کے باہر اگر کوئی بیٹھ جائے اور اُس کے گھر کے وائی فائی کے سگنلز کو بغیر اُسکی اجازت کے استعمال کرے یا اگر کسی کے گھر کی بجلی اُسکی بغیر اجازت کے استعمال کی جائے تو جس طریقے سے یہ چوری ہے بِعَینہٖ اسی طریقے سے کرپٹو جیکنگ کے متعلق مفتیانِ کرام یہ ارشاد فرماتے ہیں کہ کرپٹو جیکنگ کے اندر سب سے بنیادی مسئلہ تو یہ ہے کہ کسی بھی شخص کی اجازت کے بغیر یا غیر قانونی طور پر اس کے کمپیوٹر کو استعمال کرتے ہوئے کرپٹو کرنسی مائننگ کا عمل کیا جارہا ہے اور یہ شرعاً جائز نہیں اور یہ چوری کے حکم میں آتا ہے۔ دوسرا یہ کہ کرپٹو جیکنگ کے ذریعے کرپٹو کرنسی مائننگ کا عمل ہو رہا ہے اور کرپٹو کرنسی مائننگ کا عمل غررِ کثیر ہے لہذا یہ دوسرا شرعی محظور ہے جس کی وجہ سے مفتیانِ کرام کرپٹو جیکنگ کے عمل کو شرعاً ناجائز قرار دیتے ہیں۔

(نوٹ: ڈاکٹر مبشر کے اس کالم کا خلاصہ آئرلینڈ کے قومی ٹی وی اور ریڈیو نشریاتی ادارتی آر ٹی وی - برین اسٹورم RTÉ Brainstorm کی ویب سائٹ پر اُن کے اپنے قلم سے انگریزی میں یکم دسمبر ۲۰۲۲ کو بعنوان ?Are cyber criminals using your computer شائع ہو چکا ہے۔)

کلماتِ تشکر

میں اپنے شیخ اور استادِ محترم حضرت مولانا مفتی محمد نعیم میمن صاحب دامت برکاتہم خلیفہ مجاز حضرت مولانا محمد یوسف لدھیانوی شہید رحمتہ اللہ علیہ کا انتہائی تہہ دل سے مشکور ہوں کہ انہوں نے ہمیشہ میری حوصلہ افزائی فرمائی اور خاص طور پر اس مضمون کو دیکھا، میری غلطیوں کی اصلاح فرمائی اور مجھے اپنی قیمتی آراء سے مستفید فرمایا جس سے اس مضمون کی افادیت بہت زیادہ بڑھ گئی الحمدللہ۔ میں اللہ پاک سے دعا گو ہوں کہ اللہ رب العزت میرے اس مضمون کو امتِ مسلمہ کیلئے باعث خیر وبرکت بنائے، میری اس ادنیٰ سی کاوش کو قبول فرمائے اور ذخیرہ آخرت بنائے، آمین۔

کچھ مصنف کے بارے میں

ڈاکٹر مبشر حسین رحمانی منسٹر ٹیکنالوجیکل یونیورسٹی (MTU) آئرلینڈ کے کمپیوٹر سائنس ڈیپارٹمنٹ میں لیکچرار ہیں اور پچھلے کئی سالوں سے بلاک چین کے موضوع پر تدریس و تحقیق انجام دے رہے ہیں۔ انہوں نے ۲۰۱۱ میں یونیورسٹی آف پیرس VI، فرانس سے پی ایچ ڈی کی ڈگری حاصل کی۔ انہوں نے آٹھ کتابیں لکھیں ہیں جن میں سے دو کتابیں بلاک چین ٹیکنالوجی سے متعلق ہیں، جس میں سے ایک کتاب کو باقاعدہ ٹیکسٹ بک کے طور پر آئرلینڈ میں ماسٹرز کے نصاب کا حصہ بنایا گیا ہے۔ بلاک چین کے موضوع پر اُن کے دسیوں تحقیقی مقالے دنیا کے بہترین تحقیقی جرائد کے اندر شائع ہو چکے ہیں۔ نیز دو طالبعلموں نے بلاک چین کے موضوع پر اُن کی سُپرویژن میں پی ایچ ڈی آسٹریلیا سے مکمل کی ہے۔ وہ کئی بہترین تحقیقی مقالوں کے ایوارڈز وصول کر چکے ہیں۔ اُن کو کمپیوٹر سائنس کے شعبے میں اُن کی تحقیق کی بنیاد پر مسلسل تین سال یعنی سن ۲۰۲۰، سن ۲۰۲۱ اور سن ۲۰۲۲ میں دنیا کے ایک فیصد بہترین سائنسدانوں کی فہرست میں میں شامل کیا گیا۔